Symantec Management Platform 7.1 SP2 Release Notes

Symantec

Symantec Management Platform 7.1 SP2 Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

Symantec and the Symantec Logo, Altiris, and any Altiris or Symantec trademarks used in the product are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Symantec Management Platform 7.1 SP2 Release Notes

This document includes the following topics:

- About Symantec Management Platform 7.1 SP2
- What's new in Symantec Management Platform 7.1 SP2
- General installation and upgrade information
- System requirements
- Installing
- Known issues
- Fixed issues
- Other things to know
- Documentation that is installed
- Other information

About Symantec Management Platform 7.1 SP2

Build number 7.1.8280

The Symantec Management Platform provides a set of services that IT-related solutions can leverage. Solutions plug into the platform and take advantage of the platform services, such as security, reporting, communications, package

deployment, and Configuration Management Database (CMDB) data. Because solutions share the same platform, they can share platform services as well as data. Shared data is more useful than data that is only available to a single solution. For example, one solution collects data about the software that is installed on company computers and another solution uses the data to manage software licenses. A third solution can also use this data to help you update software. This close integration of solutions and the platform makes it easier for you to use the different solutions because they work in a common environment and are administered through a common interface.

The platform provides the following services:

- Role-based security
- Client communications and management
- Execution of scheduled or event-triggered tasks and policies
- Package deployment and installation
- Reporting
- Centralized management through a single, common interface
- Configuration Management Database (CMDB)
- Software Management Framework

When you install a solution or suite, the platform is also installed if it is not already installed.

What's new in Symantec Management Platform 7.1 SP2

In the 7.1 SP2 release of Symantec Management Platform, the following new features are introduced:

Table 1-1 List of new features

Component	Description
General	■ Symantec Help Center The Symantec Management Platform 7.1 SP2 release provides Symantec Help Center. This search-based Help system implements many Web 2.0 features, such as autosuggest and filtering. It also deploys the customized search logic that helps you get more relevant answers to your questions. ■ Symantec ServiceDesk no longer installed as a part of IT Management Suite in Symantec Installation Manager To install Symantec ServiceDesk, you must select the product separately in the product listing in Symantec Installation Manager.
Core	■ Support for Microsoft MED-V virtualization This enhancement adds the ability for Symantec Management Agents on Microsoft MED-V virtual devices to communicate through devices in NAT mode. It is now supported in 6.x or later. ■ NSE processing improvements enable faster inventory updates and consume less processing power on Notification Server and Microsoft SQL systems. ■ Registry keys can be used to change the path to Logs and the Event queue. ■ Scalability - One Notification Server now supports up to 300 task servers. ■ Support for SQL 2008 R2 SP1 ■ Support for SQL 2005 SP4 ■ Support for Windows Internet Explorer 9 in compatibility mode ■ A 5,000-seat environment was tested and documented to provide hardware recommendations and to minimize hardware expenses for SMB environments. For more information, see the IT Management Suite Planning and Implementation Guide at http://www.symantec.com/docs/DOC4827

Table 1-1 List of new features *(continued)*

Component	Description
Symantec Installation Manager	■ Ability to perform offline upgrades You can export a server's installation history and import it to an Internet-connected computer to create an installation package. ■ Log files for support packages Symantec Installation Manager lets you create and view verbose and non-verbose log files for inclusion in a support package. ■ Ability to create installation packages on Windows XP/7 computers You can now run Symantec Installation Manager on the platforms that Notification Server does not support. Examples of these platforms are Windows XP/7, but only for the purpose of creating offline installation packages. ■ Improvements to SSL configuration New options for supplying a certificate during installation. The options include **Create self-signed**, **Import**, and using a certificate available on the computer. For more information, see the *Symantec Management Platform 7.1 SP2 Installation Guide*. http://www.symantec.com/docs/DOC4798
Enhanced Console Views	■ New Software Management privileges Software Management privileges grant specific abilities to the user role. They also allow the user to perform specific tasks in the **Software** view and **Software Catalog** window from the enhanced console views. ■ Improved **Licenses** tab Improvements in the **Licenses** tab, on the **Software Product** dialog box, let you choose whether to license a software product. These improvements also let you create additional licenses for the same software product. ■ Improved **Delivery** tab Improvements in the **Delivery** tab, on the **Software Product** dialog box, let you import software packages, add software packages, and add command lines. ■ Additional search options Improvements in the **Enhanced Views Setting** dialog box let you configure search settings for the **Software** view and **Computer** view center panes (list panes). See *Altiris IT Management Suite 7.1 SP2 from Symantec Enhanced Console Views Getting Started Guide* at the following URL: http://www.symantec.com/docs/doc4858

Table 1-1 List of new features *(continued)*

Component	Description
Symantec Workflow	■ Symantec Workflow is delivered through Symantec Management Platform. ■ The Configuration and Logging Tool in Workflow Designer was renamed to **Workflow Explorer**. ■ Users can now enter platform credentials during installation, but AD credentials were removed from the installation. ■ Improvements in Active Directory synchronization let you selectively synchronize users with Symantec Workflow. ■ New import profiles and export profiles are available. ■ Symantec Workflow includes a refreshed Sharepoint component library. ■ All integration projects are now multi-generator container projects by default. ■ A new application installer is included for partners.
Software Management Framework	■ Support of virtualization package format XPF This enhancement ensures that the software catalog adds support of the default package format of Symantec Workspace Virtualization. ■ Changes in Software Management Framework Agent inventory report To prevent accidental loss of Software Management Framework inventory data, a periodical send of full inventory data ia added. For more information, see the following knowledge base article at the following URL: http://www.symantec.com/docs/HOWTO60920. ■ **Automatically generate command lines when a package is created** checkbox in **Add or Edit Package** dialog box This checkbox lets you generate appropriate command lines when a new package is added to either a new software resource or an existing software resource.

Table 1-1 List of new features *(continued)*

Component	Description
UNIX, Linux, Mac Agent	■ NSE events You can now select specific resource keys to be ignored when you generate NSE events. For more information, see the knowledge base article at the following URL: http://www.symantec.com/docs/HOWTO60919. ■ Support for 64-bit RHEL 6 A 64-bit bootstrap module is added to the solution package to support installation on the RHEL 6 64-bit platforms without a 32-bit compatibility layer. ■ Various enhancements for Client Task Agent ■ Changes in agent packaging for Mac platform ULM Agent distribution for MacOS now contains signed files (libraries, binary executables, and application bundles). Files are signed with the official Symantec certificate. ■ Support for Mac OS X 10.7.x and Mac OS X Server 10.7.x

General installation and upgrade information

You install this product by using the Symantec Installation Manager. You can download the installation files directly to your server or you can create offline installation packages.

For more information, see the *Installing IT Management Suite* chapter in the *IT Management Suite 7.1 SP2 Planning and Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC4827

See the product's documentation for information on how to configure and use it.

To perform an upgrade from version 7.1 or later, in the Symantec Installation Manager click **Install New Products**, and then choose to install this product. Do not use the **Install Product Updates** page to upgrade.

Symantec recommends that you upgrade all of the installed products to the latest version. The easiest way to achieve this is to choose to install a suite.

If you use hierarchy, you must disable hierarchy replication and upgrade all products to the latest version on each of the Notification Server computers.

For additional information about upgrading, see the **Upgrading to IT Management Suite 7.1 SP2 - Best Practices** article at the following URL:

http://www.symantec.com/docs/TECH177513

After you upgrade the product, you must upgrade the Symantec Management Agent and the plug-ins that are installed on the managed computers. Symantec recommends that you do the following:

- In the Symantec Management Console, click **Actions > Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, under **Symantec Management Agent**, locate and turn on the upgrade policies for the Symantec Management Agent.
- In the Symantec Management Console, click **Settings > All Settings**. In the left pane, expand **Notification Server > Site Server Settings**, and then locate and turn on the upgrade policies for various site server plug-ins.
- In the Symantec Management Console, click **Actions > Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, locate and turn on the upgrade policies for various plug-ins.

Symantec recommends that you configure a schedule for these policies; the default **Run once ASAP** option may not trigger the policy if this is not the first time you perform an upgrade. Also, to speed up the upgrade process, consider temporarily changing the **Download new configuration every** setting on the **Targeted Agent Settings** page to a lower value.

For detailed instructions on migrating from 6.x and 7.0 to 7.1 SP2, see the following documentation resources:

- *IT Management Suite Migration Guide version 6.x to 7.1 SP2* at the following URL:
  http://www.symantec.com/docs/DOC4742
- *IT Management Suite Migration Guide version 7.0 to 7.1 SP2* at the following URL:
  http://www.symantec.com/docs/DOC4743

System requirements

The recommended system requirements vary depending on the size of the environment. The size of the environment also affects how you configure the platform.

Symantec Management Platform 7.1 SP2 requires Windows Server 2008 R2 (64-bit) or Windows Server 2008 R2 SP1 (64-bit).

For more information, see the *Altiris IT Management Suite 7.1 from Symantec Planning and Implementation Guide* at http://www.symantec.com/docs/DOC4827.

Installing

Refer to the *Altiris IT Management Suite 7.1 from Symantec Planning and Implementation Guide* at http://www.symantec.com/docs/DOC4827.

You can also refer to the *Symantec Management Platform 7.1 SP2 Installation Guide* at http://www.symantec.com/docs/DOC4798.

Known issues

The following are known issues for this release. If additional information about an issue is available, the issue has a corresponding Article link.

For the most up-to-date information, latest workarounds, and other technical support information for this product, see the Technical Support knowledge base.

The known issues are separated into the following components:

- Symantec Installation Manager
  See Table 1-2 on page 11.
- Notification Server
  See Table 1-3 on page 11.
- Task Server
  See Table 1-4 on page 15.
- Symantec Management Agent
  See Table 1-5 on page 16.
- Software Management Framework
  See Table 1-6 on page 17.
- Data Connector
  See Table 1-7 on page 19.
- Network Discovery
  See Table 1-8 on page 20.
- Credential Manager, Connection Profiles, and the Pluggable Protocols Architecture
  See Table 1-9 on page 20.
- UNIX/Linux/Mac
  See Table 1-10 on page 21.
- Symantec Management Console enhanced console views
  See Table 1-11 on page 24.
- Administrator SDK

See Table 1-12 on page 27.

Table 1-2 Known Issues for Symantec Installation Manager

Issue	Description	Article Link
Cannot install Symantec Management Platform on a server with a previous installation of the SSDK (Altiris Solution SDK).	The Notification Server computer does not install on a server that also has the Solution SDK (SSDK) installed on it. If you attempt to install in this environment, the installation fails. Uninstall the SSDK before you install Symantec Installation Manager (SIM) and solutions.	TECH175688
Some licenses do not appear correctly on the **Product Licensing** page.	If you install IT Management Suite and do not apply licenses, Symantec Installation Manager (SIM) should apply extended trial licenses (30 days). However, if Symantec Installation Manager cannot contact the licensing server, it applies a regular trial license (seven days). The **Product Licensing** page shows these as regular trial licenses rather than the extended trial licenses.	TECH176492
Uninstall leaves files and folders.	After you uninstall the Symantec Management Platform products, many files, registry keys and values, and directories are not uninstalled. You can remove these items with the SmpZap command line utility. The Article ID link accesses a knowledge base article with instructions for using this utility.	TECH42647

Table 1-3 Known Issues for Notification Server

Issue	Description	Article Link
In certain instances you cannot export a policy to a local folder with full permissions on a Windows 2008r2 x64 server computer.	This limitation occurs if you use a console that is open on localhost and if IE ESC (Enhanced Security Configuration) is turned on for Administrators. When you attempt to save such a policy to a local folder with full permissions, the following message is displayed: "You don't have permission to save in this location... Would you like to save in the My Documents folder instead?" This issue occurs only when Internet Explorer ESC (Enhanced Security Configuration) is turned on for Administrators. To work around this issue, turn off Internet Explorer ESC.	TECH176433

Table 1-3 Known Issues for Notification Server *(continued)*

Issue	Description	Article Link
Abnormally high CPU and Memory usage for `w3wp.exe` on Windows 2008 64-bit.	Occasionally the **www publishing** service `w3wp.exe` process causes very high CPU and Memory usage. It can cause the computer to stop responding. It is a problem on low-end Windows servers with single core processors. To work around this issue, restart the **www publishing** service.	TECH176493
Emergency policy update does not work properly in a hierarchy environment.	The emergency policy update does not work in a hierarchy environment if the **Quick Delivery** task is used in the **Managed Software Delivery** policy. This issue occurs if you create a **Managed Software Delivery** policy on the parent Notification Server and then target one client on the parent Notification Server and another on the child Notification Server. After you initiate the emergency policy update, the **Managed Software Delivery** gets executed successfully on the client on the parent Notification Server. It does not get replicated on the child Notification Server.	TECH176438
Problems can occur when you try to control the installation schedule for plug-ins.	Some policies that use scheduled time zones are handled incorrectly on the client side. This problem occurs if the server and the client time are set to different time zones or to a different time. If scheduled resource membership updates are performed on a server with its clock set to a future time, then new resources are not added. The resources are not added until the next resource membership update is performed. If you then set the clock on the server back to the current time, a new problem arises. The next resource membership update cannot be performed because the current time is less than the previous update time. For example, the agent rollout policies that are based on SWD rely on the Task Scheduler. The rollout policy page uses the policy scheduling control, which provides more capabilities than the Task Scheduler supports. Among other things, the Task Scheduler does not support the use of time zones.	TECH176442

Table 1-3 Known Issues for Notification Server *(continued)*

Issue	Description	Article Link
When you right-click **Hierarchy Management**, an error message appears and you cannot set up Hierarchy.	When you right-click **Hierarchy Management**, the following error message appears: `[3]: Object does not support property or method 'clear' [-2146827850]` This error appears only if you use Internet Explorer 9 with the enhanced security enabled to access the Symantec Management Console through HTTPS. The way IE9 handles ActiveX controls causes this problem. To work around this issue, perform the following steps: 1. In Internet Explorer 9, on the **Tools** menu, click **Internet Options**. 2. In the **Internet Options** dialog box, on the **Advancecd** tab, uncheck the **Do not save encrypted pages to disk** box.	TECH172928
If Notification Server is installed on a non-default HTTPS port, it is impossible to install or use an agent using an ISA proxy server.	If you use a non-default HTTPS port (for example, 1111) to install Notification Server, you cannot install or use an agent through an ISA proxy server. The ISA proxy server requires additional configuration.	TECH176496
You must restart of Notification Server services after reconfiguring the database from the console.	When you upgrade from Dell Management Console 1.1 to Dell Management Console 2.0, if you connect to the old database on the **Database Settings** page in the console, you must do a restart. You must restart Notification Server services before you can execute any tasks. Symantec recommends that you connect to your restored 7.0 CMDB from the **Database Configuration** page in Symantec Installation Manager and not from the console.	TECH176497
Creating a new automation policy creates an error, and a warning-level message is logged.	When you create a new automation policy, an error is generated and warning messages are logged. However, after you create the policy you can load it, change settings, and save it without the error recurring.	TECH176444

Table 1-3 Known Issues for Notification Server *(continued)*

Issue	Description	Article Link
The **Create Resource Targets** privilege is not currently used.	Any user who has the permission **Apply to Resource Targets** can create resource targets. Enabling or disabling the Create Resource Targets privilege has no effect. The menu path is **Settings > Security > Roles**. In **Roles**, click the **Privileges** tab. If you want to prevent a user from creating resource targets, remove the **Apply to Resource Targets** permission from that user. Removing this permission means that the user cannot open the resource selector dialog box.	TECH176445
Attempts to access the Symantec Management Console using the Fully Qualified Domain Name in the console URL may fail with an error message.	If the Symantec Management Console is set up to use a non-default port, you may see an exception error in the following situation: you try to add computers on the **Agent Push** page of the console by using the FQDN (non-localhost). The following error message is displayed: Data for the page you are currently viewing has expired. Workaround: Use the appropriate IP address in the console URL rather than using the FQDN.	TECH121988
Replicated Symantec Management Agent Settings - Targeted policy can be edited or deleted on child Notification Servers.	If you replicate the Targeted Agent Settings policy to child Notification Servers, the replicated policy is editable on the children. The path in the Settings tree is: **Settings > Agents/Plug-ins > Symantec Management Agent > Settings > Symantec Management Agent Settings - Targeted**. This replicated policy should not be editable. Replicated System Policies should be read-only on child Notification Servers, and you should not be able to modify or delete them. Any changes that you make to this policy on a child Notification Server is overwritten on the next replication schedule. On that next schedule, the same policy is replicated again from the parent.	TECH176500

Table 1-3 Known Issues for Notification Server *(continued)*

Issue	Description	Article Link
Drill-down reports fail when the drill-down targets a remote Notification Server that uses a non-default port.	If you have a hierarchy of Notification Servers, some reports display summary data for each Notification Server. These reports let you drill down into the results. To drill down you click the appropriate row in the results grid for detailed data about a particular Notification Server. However, if a Notification Server is installed to a non-default Web site and port, its summary data is displayed correctly in the summary report. Any attempt to drill down to display the detailed data fails. A new browser window opens to display the report results, but it contains a Server Error message saying that the resource cannot be found.	TECH46377
Low policy updating performance for large client infrastructure.	It may take a long time to load the **Select computers** dialog box while you update the policies in some instances. This low performance can occur for an infrastructure that has a large number of client computers. Consequently, warning messages are displayed because the update time exceeds the process timeout period.	TECH176502
Data Connector fails to import some values from LDAP.	If the Active Directory attribute contains multiple values, the Data Connector import rule only imports the last value of the attribute.	TECH176504
The **Purging Maintenance** page may take several minutes to load.	In Symantec Management Console, the **Settings > All Settings > Settings > Notification Server > Purging Maintenance** page may take several minutes to load.	TECH171024

Table 1-4 Known Issues for Task Server

Issue	Description	Article Link
Sample task **Delete Temporary Files** does not delete files on all operating systems.	The sample client task **Delete Temporary Files** does not delete any files on Windows Vista, 7, or 2008 operating systems. The task does not delete files on these operating systems for all user profiles because it looks for the files in the wrong location.	TECH160710
The initial use of ".\username" causes any script tasks that are specified as Machinename\username to fail with the error 'Unable to open the file.'	This error is due to a profile loading problem. This issue applies only to some operating systems, such as Window XP SP2 and Windows 2003. It does not apply to Windows 7 or to Windows Vista Ultimate SP2.	N/A

Table 1-4 Known Issues for Task Server *(continued)*

Issue	Description	Article Link
Task Server task runs even though **Allow other tasks to run while running this task** is unchecked.	If you create a task and uncheck the **Allow other tasks to run while running this task** option, other tasks can still run.	N/A
Task Server needs to be restarted after a new database has been created.	When you create a new database, you need to restart Task Server (Altiris Object Host Service) from the Windows service console. This restart is required to make the previously scheduled Patch Management import task run.	TECH45090
Tasks that are contained within jobs must be migrated separately.	When you migrate a job from 6.0 to 7.1, you also need to migrate the associated tasks. The tasks that are included in the job are not migrated automatically with the job.	N/A

Table 1-5 Known Issues for Symantec Management Agent

Issue	Description	Article Link
Cannot push the Symantec Management Agent to a Windows XP client computer with default configuration.	Pushing the Symantec Management Agent from a Notification Server to a client computer that has Windows XP with a default configuration causes the installation to fail. Workaround: Disable Windows XP simple file sharing. 1. In Windows, click **Start**, and then click **My Computer**. 2. On the **Tools** menu, click **Folder Options**. 3. Click the **View** tab. 4. In the **Advanced Settings** section, make sure that the **Use simple file sharing (Recommended)** check box is not checked, and then click **OK**.	TECH176452
Image creation fails if teaming is configured for network controllers.	Deployment Solution does not work in environments where network adapters are teamed, because Symantec Management Agent does not detect adapters if teaming is configured.	N/A
Cannot install Symantec Management Agent plug-ins if the Windows temporary folder is not configured correctly.	If a Temp folder is not configured correctly or points to a folder that does not exist, the installation task fails.	TECH176454

Table 1-6 Known Issues for Software Management Framework

Issue	Description	Article Link
An incorrect association results for two Notification Servers in a hierarchy in a certain situation.	Consider two Notification Servers in a hierarchy. This problem occurs if the parent and child have the same software resource imported but have different software products associated with the resource. When you perform replication from the parent to the child under these circumstances, the affected software resource on the child shows an incorrect association. Instead of showing one association from the parent Notification Server, the affected software resource shows two associations: one from the parent and one from the child. Workaround: Perform a second replication from parent to child. After this second replication, the affected software resource shows the correct association.	TECH176457
The **Software Data Provider Status** report does not show results.	When you add or run data providers and then try to view the status of the data providers using the **Software Data Provider Status** report, the report does not show results.	N/A
A Managed Software Delivery policy only logs off a single user session when there are multiple active or disconnected terminal sessions.	The **Log off user** option in the **Managed Software Delivery** policy logs off only a single session rather than all sessions when multiple sessions are active. For more information, see topics on Results-based actions settings in Software Management Solution in the *Altiris™ Software Management Solution from Symantec™ User Guide* at the following URL: http://www.symantec.com/docs/DOC4661 Workaround: Use the **Log off** option available with the **Restart Computer** task to successfully log off every session.	N/A
The **Windows Language** applicability rule does not work properly when **Neutral** language is selected.	The applicability check status should evaluate as **Detected** and the software installs successfully. Instead, the applicability check evaluates as **Not Detected** and the software is not installed.	N/A

Table 1-6 Known Issues for Software Management Framework *(continued)*

Issue	Description	Article Link
Software Components do not replicate using **Replicate Now**.	Replication of software components does not work from a parent or child Notification Server when you use **Replicate Now** in the following situations: ■ In the **Software** view, when you use the right-click menu **Hierarchy > Replicate Now** on either **Software Releases** or **Software Updates**. ■ In the **Manage** menu, select **All Resources**, and right -click on a software component. From the right-click menu select **Hierarchy > Replicate Now**.	N/A
An incorrect version is reported for Microsoft Internet Explorer 8.	When you run **Collect Full Inventory** on a client computer with Microsoft Internet Explorer 8 installed, the version is incorrectly displayed in the inventory report.	N/A
If an externally initiated restart is performed during Managed Software Delivery, then the software that is installed after the restart fails.	If an externally initiated restart is performed during Managed Software Delivery, then the software that is installed after the restart fails. The reason the installation fails is that the software starts to install while a user logoff is still pending.	N/A
Software resource associations of a software component to file are not present if an application is installed on a client computer for a specific user.	Consider a software application that is installed on a client computer by a specific user. A **Collect Full Inventory** is then run for that client after a different user logs in to this computer. In this situation, the resource associations of the software component to file is lost for this software resource. The problem occurs because Software Discovery tries to load values from a user-specific registry. However, it is unable to load those values because the specific user is not logged on.	N/A
Files in the **File Inventory** tab are overwritten if a software resource is moved to **Managed Software** and metering is turned on for this software resource.	Files in the **File Inventory** tab are overwritten if a software resource is moved to **Managed Software** and metering is turned on for this software resource.	N/A
Software resource names mapping is discarded during the IT Management Suite upgrade.	The changes that are made to the Known As mapping of the software resource are discarded during the upgrade from IT Management Suite 7.1 to IT Management Suite 7.1 SP2.	

Table 1-6 Known Issues for Software Management Framework *(continued)*

Issue	Description	Article Link
Quick Delivery tasks fail to execute by timeout when maintenance window is set up on clients.	If you create a Quick Delivery task and the task times out before the maintenance window is activated on the client, the task fails. By default, a task times out after 300 minutes. On the **Task options** tab of the Advanced settings, you can change when a task ends.	N/A
A Managed Software Delivery policy runs too often.	A Managed Software Delivery policy that targeted a user and was scheduled to run only once runs each time the targeted user logs on.	N/A
Problems with the applicability check in a Managed Software Delivery policy.	If a Managed Software Delivery policy delivers two software resources and the second software resource is dependent on the first software resource, the applicability check for the second resource fails. The failure occurs because this check runs before the first software resource is installed.	N/A
Applications with large installation paths fail to execute.	With a Managed Software Delivery policy or Quick Delivery task, applications with large installation paths fail to execute.	TECH133459

Table 1-7 Known Issues for Data Connector

Issue	Description	Article Link
The CMDB rules **Update Mode** changes when the rules are migrated from 6.x to 7.1.	The migration wizard changes the CMDB rules **Update Mode** from **Append** to **Update** even if it is originally set to **Append** in 6.x. The rules migrate and work. However the way they function is not the same. A rule that has its **Update Mode** set to **Append** in 6.x, has after the migration to 7.1 changed its mode to **Update**.	N/A

Table 1-7 Known Issues for Data Connector *(continued)*

Issue	Description	Article Link
Collection migration issue.	Data connector v6.x can have **CMDB Rules, Resource Export Rules**, and **Bulk Resource Export Rules** which use collections. During the migration process, the collections used by those rules are converted to resource targets. The resource targets that are converted from the collections should contain the same memberships as the legacy collections. In this release, the conversion process is not functioning properly: the resource targets that are converted from the legacy collections do not contain memberships. To work around, you need to re-create the resource targets for those rules by using the legacy collections to make them work properly.	TECH176458

Table 1-8 Known Issues for Network Discovery

Issue	Description	Article Link
Exception in Notification Server log during upgrade with hierarchy.	When running the hierarchy differential replication schedule in certain upgrade scenarios, you may get exceptions such as: "Incompatible columns in DataClassAttribute. Error:Class Name: VM Guest" in the Notification Server computer log. Break the hierarchy before upgrading. Then, upgrade both parent and children before re-joining.	

Table 1-9 Known Issues for Credential Manager, Connection Profiles, and the Pluggable Protocols Architecture

Issue	Description	Article Link
Altiris object host service crashes when it runs the VMM inventory task on multiple hypervisors.	To work around this issue, run the VMM inventory task one hypervisor at a time.	N/A
WMI, WSMAN, and other monitoring plug-ins become unavailable if multiple web-service identities are used.	You must ensure that you remove multiple identities if you choose a custom Web site.	TECH142631

Table 1-10 Known Issues for UNIX/Linux/Mac

Issue	Description	Article Link
Package server agent 6.x on a Linux server is not upgraded automatically.	If you migrate to ITMS 7.1 SP1 and you have package server agent 6.x on a Linux server, the package server agent is not automatically upgraded to 7.1 SP1. This issue occurs because the Legacy Linux package server agent upgrade rollout policy is not available. The workaround is to complete the following steps: ■ Upgrade the UNIX/Linux/Mac Agent from the 6.x version to the 7.1 SP1 version on the package server. ■ Add the Linux Server that has the package server agent 6.x to the resource target of the Linux package server agent Upgrade policy. When the policy is received on the package server, the package server agent is upgraded to the 7.1 SP1 version. ■ Send basic inventory from the package server. After the execution of the "NS.Package Server Status Event Capture Item {f85fe5d9-005a-40ac-b213-944b496405fe}" scheduled task, the Linux Package Service is automatically created on the **Site Server Management** page. The Linux Package is then ready to work with Symantec Management Platform 7.1 SP1 and your managed clients.	N/A
ULM Agent 7.0.4541: incorrect time is returned by the agent after manual change of time zone on client systems.	After you make a time zone change on a UNIX/Linux/Mac client, the change may not affect running services until after you restart the client system.	TECH153660
HttpdIntegration does not properly parse Apache config file with SSL and custom.	Known limitations exist on supported Apache configurations for the computer that is intended as a package server candidate. Please avoid using complex Apache configurations on such computers.	N/A
HttpdIntegration does not use apache_config_location parameter in client.conf.	Known limitations exist on supported Apache configurations for the computer that is intended as a package server candidate. Please avoid using complex Apache configurations on such computers.	N/A

Table 1-10 Known Issues for UNIX/Linux/Mac *(continued)*

Issue	Description	Article Link
You can enable a package server password when **Publish HTTP codebase** is enabled.	A certain security risk exists if you disable anonymous access to a Linux package server in HTTP mode. Linux package servers support only "basic authentication". Consequently, passwords are sent in plain text. Use either HTTPS or keep anonymous HTTP access for a Linux package server.	N/A
Impossible to reset proxy settings by `AeX-configure -iconfigure`..	You cannot reset enabled proxy settings from the client. Disable proxy settings by updating the corresponding configuration policy in the Symantec Management Console.	N/A
Time zone, OS language, Primary User, and host id are not found under Resource Summary.	Some basic inventory information may not be reported for certain ULM systems (Solaris, HP-UX, and RedHat).	N/A
If you select a service action for AIX `inittab` services in a UNIX/Linux/Mac Service Control task, the task fails with an error message.	The AIX `inittab` service does not support any of the actions that are available in the **Service Action** drop-down list. When the AIX `inittab` service is checked, the **Service Action** field should be grayed out and not selectable. At present this field is (incorrectly) functional in the Symantec Management Console. To avoid errors in your Service Control task, set the **Service Action** field to **No action**. This action prevents any attempt to execute Start, Stop, Restart, or Get Status commands for AIX `inittab` services. Note that currently the No action setting is incorrectly processed and cannot be used for task creation. As a result, all Service Control tasks that are created for the `inittab` service control system are reported as failed. The error message “Missing or invalid service action” is displayed. This message appears regardless of whether the specified process or service was successfully modified.	TECH46454
You cannot use an upgrade policy to upgrade the Symantec Management Agent for UNIX and Linux to version 7.1 from version 6.2.1378 on HP-UX computers with IPv6 enabled.	The simplest way to work around this issue is to upgrade to Symantec Management Agent 7.1 using the Push installation method. Alternatively, you can disable IPv6 on the target computer.	TECH42029

Table 1-10 Known Issues for UNIX/Linux/Mac *(continued)*

Issue	Description	Article Link
ULM agent does not support NTLMv2 protocol for security connection with the Notification Server computer.	Currently, NTLMv2 on UNIX/Linux/Mac computers is not supported. Several workarounds exist, but most of them lead to security degradation. The agent cannot access protected URLs (such as http://smp-wn2008x64-5/Altiris/TaskManagement/CTAgent/GetClientTaskServers.aspx). In the client log, you can see a warning message like "Attempt for url http://smp-wn2008x64-5/Altiris/TaskManagement/CTAgent/GetClientTaskServers.aspx?resourceGuid={7EA6503B-1A60-4F48-BE77-34C7D2B861AB} returned 2147554187, Post failed, HTTP error: 401". Possible workarounds are as follows: 1) Install Notification Server on HTTPS (if it is already installed). In ULM-specific targeted agent settings, you can specify an Alternate Notification Server URL and set the protocol to HTTPS. Leave the remainder intact. Then refresh policies on the agent. 2) Use anonymous access to the Notification Server. User should manually enable "anonymous authentication" and disable "windows authentication" on all Notification Server nodes in the IIS management console. Perform the same operation on all site servers. Lower "LAN Manager authentication level" in group policies to a level that supports NTLM authentication. Note that if you use domain accounts, then this operation should be performed on Notification Server, site servers, and the domain controller. If it is impossible to lower the security level on the domain controller, but it is okay for Notification Server and site servers, then it is possible to use the local account as Notification Server "access credentials." Note that in this case the same local user should exist on all Notification Server computers.	

Table 1-10 Known Issues for UNIX/Linux/Mac *(continued)*

Issue	Description	Article Link

An unusual character limitation occurs with a script task on SLES.	A custom command metric with the following command line returns an incorrect value on SLES 10:
	`ps -ef | grep -v 'grep' | grep -c -i -w "chssrvInfoServerapp01mgtNode01Cell"`
	The value that is returned when executed within the OS shell is "1," but the metric returns a value of "0." This value is to monitor if a process is running, but something interferes with the command execution of the metric. The cause is a character limitation of 32 characters of the desired process name (not a character limitation of the entire command-line syntax).
	The command returns either a "1" or a "0"; therefore, the character length of the process name should not be an issue, but it is.
	If you configure the command line of the metric as follows, it returns the correct value:
	`ps -ef | grep -v 'grep' | grep -c -i -w "chssrvInfoServerapp01mgtNode01Ce"`
	Note: This issue does not appear to exist on RHEL computers.	

Table 1-11 Known Issues for Symantec Management Console enhanced views

Issue	Description	Article Link
If you click **Help > Context**, different SymHelp content may be displayed than if you press F1.	Symantec Management Platform pages that are made in Silverlight cannot determine where the focus is on the ASPX page. As a result, different SymHelp topics may be displayed when you click **Help > Context** rather than press F1.	N/A

Table 1-11 Known Issues for Symantec Management Console enhanced views *(continued)*

Issue	Description	Article Link
Issues arise when the option to use Input Method Editor (IME) is checked.	On the **Enhanced Views Settings** dialog box, you can check an option to use Input Method Editor (IME). This option lets you input double-byte characters in these views. When you check the option to use IME, you may encounter the following issues: ■ In a dialog box, to move the focus from the previous text box, you have to double-click the new text box. ■ A text box may appear to float on the page when you move a dialog box. A text box may remain after you close a dialog box. The text box disappears when you click anywhere on the screen. The enhanced views use Silverlight. For IME, the HTML fields are overlaid on the Silverlight pages to accept the double-byte characters. In most cases, the data entry works as if you used the page without the IME support. However, in other cases such as with dialog boxes, the HTML fields are not anchored to the dialog box. ■ You may encounter some abnormal formatting. ■ An error message concerning errors on a Web page may appear.	
When the custom schedule of the default policy **Collect Delta Software Inventory** is updated, an exception is thrown.	When the custom schedule of the default policy **Collect Delta Software Inventory** is updated, an exception is thrown. This issue occurs when you update the custom schedule and run the policy more than two times. To access the **Collect Delta Software Inventory** policy, do the following: ■ On the **Manage** menu, click **Policies**. ■ In the left pane, click **Discovery and Inventory > Inventory > Collect Delta Software Inventory**.	N/A
Software metering is not enabled automatically.	This issue occurs when you work in **Symantec Management Console > Manage > Software**. To meter software, you must manually identify the software program that you want to track. In certain cases you see a warning that instructs you to enable metering. Note that you can only meter software if you have Inventory Solution (CMS, SMS, or ITMS) installed.	N/A

Table 1-11 Known Issues for Symantec Management Console enhanced views *(continued)*

Issue	Description	Article Link
When you access the console through an additional non-default port, the Silverlight interface immediately errors out.	When you access the console through an additional non-default port, the interface immediately throws errors because Silverlight does not support additional non-default ports. Open Internet Information Services (IIS) Manager and click **Default Web Site**. In the **Action** pane, click **Bindings > Add** to add another site binding. Add another non-default port. Adjust the settings, if necessary. Click **OK** to apply changes. Use the additional non-default port to access the console. The Silverlight user interface immediately errors out. Workaround: Use only one non-default port and remove the other non-default port.	TECH167479

Table 1-11 Known Issues for Symantec Management Console enhanced views *(continued)*

Issue	Description	Article Link
Using additional search criteria in the **Computers** view may yield unexpected results.	This issue occurs when you work in **Symantec Management Console > Manage > Computers**. Click **All Computer Views > All Computers**. Click the double-arrows next to the search field in the center pane (list pane). Click **Add Search Criteria > Add Custom Criteria**. In the **Add Custom Criteria** dialog box, click **DataClasses > Logical Device**. Then click **Columns > Logical Device > Model**. Click **OK**. Enter the Google operators in the search field and click the search symbol. The search does not work. A workaround is to complete the following steps: ■ Click **Symantec Management Console > Manage > Computers** and then click **All Computer Views > All Computers**. ■ Click the double-arrows next to the search field and then click **Add Search Criteria > Add Custom Criteria**. ■ In the **Add Custom Criteria** dialog box, click **DataClasses > Logical Device**. Then click **Columns > Logical Device > Model**. Then, click **OK**. ■ Click **Add Search Criteria > Device ID**. In the **Device ID** field, type `//SYS/COMPUTER:0`. ■ In the search field, enter the Google operators and click the search symbol. The search works and yields the correct results. **Note:** This workaround may not work for virtual machines. The **Device ID** is specific to physical computers.	N/A

Table 1-12 Known Issues for Administrator SDK

Issue	Description	Article link
Default parameters are used when you run a report with non-default parameters.	RunReportWithParameters does not use the parameters that are passed to it. Instead, it uses the default parameters. The workaround is to use the Symantec Management Console to clone the report that you want to run. Edit the default parameters of the cloned report, set them to the values you want to run, and save the cloned report. Then run this new report from the ASDK.	N/A

Table 1-12 Known Issues for Administrator SDK *(continued)*

Issue	Description	Article link
Two different resource items have the same name in the CMDB when Symantec Management Platform is installed on a virtual machine.	When Symantec Management Platform is installed on a virtual machine (VM), two different resource items that have the same name are added to the Configuration Management Database (CMDB). One resource item represents the physical computer hosting the VM, and the other resource item represents the VM itself. The creation of two different resource items with the same name is by design. This naming issue affects the functioning of the following two APIs in the SWDSolnAdvertisementManagement library in the Altiris.ASDK.NS.SoftwareDelivery namespace: ■ GetAdvertisementExStatusByResourceName ■ GetAdvertisementExRunTimeByResourceName For the ASDK's software delivery functionality to work correctly, these two APIs need to retrieve the item representing the VM. However, they may instead retrieve the item of the same name representing the physical computer. The workaround is to retrieve the VM item using its GUID rather than its name, with the APIs GetAdvertisementExStatusByResourceGuid and GetAdvertisementExRunTimeByResourceGuid.	N/A
ASDK log files are always installed at %ProgramFiles%\Altiris\ASDK\Logs.	When Symantec Management Platform is installed to a custom location other than the default path, the ASDK log files are still created under the Logs directory of the default path. The default path is %ProgramFiles%\Altiris. The path to the Logs directory is %ProgramFiles%\Altiris\ASDK\Logs. The logs can still be accessed and read under that directory.	N/A
You cannot automate the addition of role privileges to right-click privileges or the removal of role privileges from right-click privileges.	SecurityManagement.AddRolePrivileges and SecurityManagement.RemoveRolePrivileges do not work on right-click privileges. An automated workaround using the ASDK currently does not exist. However, right-click privileges can be added to a role and removed from a role using the Symantec Management Platform item update process.	N/A

Table 1-12 Known Issues for Administrator SDK *(continued)*

Issue	Description	Article link
You cannot use the ASDK to set a schedule on a policy item.	ItemManagement.SetItemsSchedule does not successfully set a schedule on a policy item. Currently a workaround using the ASDK does not exist.	N/A

Fixed issues

The following are the previous issues that were fixed in this release. If additional information about an issue is available, the issue has a corresponding Article link.

The fixed issues are separated into the following components:

- Symantec Installation Manager
  See Table 1-13 on page 30.
- Notification Server
  See Table 1-14 on page 30.
- Task Server
  See Table 1-15 on page 32.
- Symantec Management Agent
  See Table 1-16 on page 34.
- Software Management Framework
  See Table 1-17 on page 35.
- Credential Manager, Connection Profiles, and the Pluggable Protocols Architecture
  See Table 1-18 on page 36.
- UNIX/Linux/Mac
  See Table 1-19 on page 36.
- Symantec Management Console enhanced console views
  See Table 1-20 on page 37.

Table 1-13 Fixed issues for Symantec Installation Manager

Issue	Description	Article link
Unable to apply additional licenses to some products.	If pcAnywhere or Deployment Solution is installed with 100 licenses applied and you try to apply an additional 1,000 licenses, the licenses are not applied. The error message indicates that you need to apply licenses with a later date over the existing licenses.	TECH133385
SQL Server name does not populate in the **Database Configuration** page during installation.	When no network is enabled, the SQL Server name does not get populated automatically on the **Database Configuration** page.	N/A
Symantec Installation Manager unable to find the product listing file.	If you extract an installation package to a non-default location, Symantec Installation Manager is not able to find the product listing file. The product listing file is not extracted to the location where Symantec Installation Manager looks for it. For example, if you extract the installation package to drive E, Symantec Installation Manager looks for the product listing at E:\Altiris\Symantec Installation Manager\Installs\Altiris\symantec.pl.xnl. To resolve this issue, have Symantec Installation Manager look for the product listing file at E:\Components\symantec.pl.xml.	TECH176455

Table 1-14 Fixed issues for Notification Server

Issue	Description	Article link
Duplicate **Symantec Management Agent for Windows - Uninstall** policy is created.	If you upgrade from Symantec Management Platform 7.0 to Symantec Management Platform 7.1 SP1, a duplicate of the **Symantec Management Agent for Windows - Uninstall** policy is created. Check the creation date of each policy and keep the policy that was created before the upgrade. To check the policy's creation date, click **Properties** on the policy's right-click menu. You can delete the other policy.	N/A
Client computer cannot download packages with a long path depth.	If a software package has a path depth longer than 256 characters, a client computer cannot download the file.	N/A

Table 1-14 Fixed issues for Notification Server *(continued)*

Issue	Description	Article link
When you select certain resource targets, an error message appears.	When a user selects a resource target, the following error message is displayed: The data could not be loaded. This error occurs when the user is a member of a role that does not have Read permission to the resource target's parent folder or to the target.	TECH176463
Custom filters in reports are not migrated completely after an upgrade.	If you upgrade from Symantec Management Platform 7.0 MR4 to Symantec Management Platform 7.1 SP1, custom filters in reports are not migrated completely. After the upgrade, check the reports to verify that the parameters of the custom filters are set correctly.	N/A
Description column of the software bulletin **Details** report is empty after an upgrade from IT Management Suite 7.0 SP2 MR2.	If you upgrade from IT Management Suite 7.0 SP2 MR2 to 7.1 SP1, the **Description** column of the software bulletin **Details** report is empty until you change the width of the column. To access this report, on the **Reports** menu, click **All Reports** and then navigate to **Software > Patch Management > Software Bulletins > Software Bulletin Details**.	N/A
Right-click menu item does not pass substitution parameters from within a virtual window.	This issue occurs if you create a right-click action item that passes a parameter to a URL that is called. If you configure it to open in **Virtual Window**, the parameter fails to be passed. If you configure it to open in **New Window** instead, it is passed.	N/A
Active Directory role and user import fails to import all the users from the targeted groups.	She security changes in Symantec Management Platform 7.1 require Active Directory import rules to be used to import large numbers of users so they can access pages in the console. The Active Directory import sometimes fails to complete the import.	N/A
Resource Manager summary page is slow to load.	The Resource Manager summary page for a computer resource takes a long time to load. It can sometimes take up to 30 seconds for the page to load.	N/A
The item picker for **Item Replication Rule** times out before it can load.	This issue occurs when you create a new **Item Replication Rule** or edit an existing rule and then click **Items** to choose the items that should be replicated. The item picker runs for up to 10 minutes without loading any items.	N/A

Table 1-14 Fixed issues for Notification Server *(continued)*

Issue	Description	Article link
Importing using Data Connector shows incorrect behavior.	If you use Data Connector to import data and have one null field that updates a populated field, this field is not updated to null in the database.	N/A
The **Active Directory Import** rule does not import security group membership unless you run a **Full Update** schedule.	A security group membership import should add the users recently added to a security group to the filters that are created for that group. The import does not work when the **Update/Differential** import is run. It only works when the **Full Import** schedule is run.	N/A

Table 1-15 Fixed issues for Task Server

Issue	Description	Article link
Script tasks that are set to run as a specific user eventually fail.	When a script task is set to run as a specific user, the discretionary access control list (DACL) grows with every call. The DACL eventually hits the 2K limit and the task fails.	N/A
Task Server unable to run tasks using 7.0 Task Servers after you upgrade to Symantec Management Platform 7.1.	After you upgrade to Symantec Management Platform 7.1, you must upgrade your 7.0 Task Servers before you can use them to run tasks.	N/A
Changing the tickle port in the config file and the user interface does not change the port.	If you change the tickle port under **Site Server** settings or in the config file from the default of 50123, the change is not made. The server continues trying to open 50123 which causes the following error to appear in the log: Unable to connect to tickle server.	N/A
The user interface limits the number of conditions that can exist in a single job.	Due to a console user interface limitation, there is a limit to the number of conditions that can exist in a single job. Altiris.WebControls.SearchSelectControl has a default limit of 20 items. Only 20 task outputs can be displayed.	N/A
Clean Task Data and **On-Demand Cleanup Task** fail to run.	**Cleanup Task Data Daily** and **On-Demand Task Cleanup** fail to maintain the maximum number of task instances. Overall performance is degraded due to the continuous increase of task instances.	N/A

Table 1-15 Fixed issues for Task Server *(continued)*

Issue	Description	Article link
Tasks that run CMD, JS, VB, and PowerShell scripts cannot be run in a Deployment Solution PXE environment.	When these tasks are run, they check if the resource is in the **All windows computers** filter. The Deployment Solution PXE Boot environment is not included in this filter. However, most Deployment Solution jobs include tasks of these types. As a result, you cannot run the Deployment Solution jobs on new computers or on the computers that have booted into the PXE environment.	N/A
Task Server agent cannot register when the Altiris Connectivity Credentials (ACC) are in use.	If you have a low-privileged ACC account in your environment, the Task Server attempts to use this account's credentials when it communicates with Notification Server. Using the ACC breaks the Task Server registration because it cannot access the item it needs to determine to which site server an endpoint belongs. The task server should use high-privileged application identity account credentials when it communicates with Notification Server.	N/A
Task status messages lost.	Task status messages are not queued on the agent like normal events. They are only sent once, when they are created. If any connection issues occur with the Notification Server computer at the time of creation, the issues are lost.	N/A
The task client does not automatically connect to the server when it uses a VPN connection.	The task client does not automatically connect to the Notification Server computer after a VPN is enabled. The agent detects that the VPN is connected and tries to connect to the server, but it fails. You must restart the Symantec Management Agent to make it connect to Notification Server.	N/A
Task run-instances are replicated to all child nodes in a hierarchy.	Any task that is scheduled to run on a client of a child server in a hierarchy is sent to that child and to the other children in the hierarchy. The task fails on all child servers except the one to which the client belongs.	N/A

Table 1-15 Fixed issues for Task Server *(continued)*

Issue	Description	Article link
Jobs with closed conditional loops cause the console to time out, and the task cannot be scheduled.	If you create either a job that calls back to itself or another job that calls back to the first job, the console stops responding. Then, the task cannot be scheduled or deleted. In addition, the application pool that is assigned to the task stops. It stops all Notification Server activities by default and does not allow access to the console until the application pool is restarted.	N/A
Client Task Agent may lose task status.	Client task status is lost if the Task Server is not available when the Client Task Agent tries to send the status. The status cannot be restored during the given timeout.	N/A

Table 1-16 Fixed issues for Symantec Management Agent

Issue	Description	Article link
The Symantec Management Agent push fails when you check **Download agent package from closest Package Server**.	If you try to push the agent to a computer and select the option **Download agent package from closest package server**, the agent is not downloaded from the nearest package server in the subnet. Either the push fails or the agent is downloaded from the Notification Server computer.	N/A
An error can occur when you try to push the Symantec Management Agent to a client computer.	When you try to push the Symantec Management Agent to a client computer, the following error message may appear: Failed to open the Service Console Manager on WM18177.wm-ag.ger. Return value=0, Error:80070005.. This error can occur if your Symantec Management Platform Application ID does not have local administrator rights on the client computer and you have specified domain admininistator credentials for the push. Notification Server Application ID account fails to log on, even though you have specified a different account for the push.	TECH169433
Setting a blockout on startup can prevent policies from running.	If you disable communication at startup for the Symantec Management Agent and then deliver policies while the agent is in a blockout, the policies do not run. The policies do not run until the agent service is restarted manually. A restart of the client computer does not solve the issue because communications are disabled on startup.	N/A

Table 1-16 Fixed issues for Symantec Management Agent *(continued)*

Issue	Description	Article link
The Symantec Management Agent does not resume functions after agent blockout period has expired.	The Symantec Management Agent does not resume functions and download packages or run them after the agent blockout period has expired. You must restart the agent services.	N/A
Software Delivery Policy closes documents without saving.	The issue occurs when you deliver a Software Delivery Policy with the **Force running applications to close** option disabled to a client running Windows 7. As a result, all open documents on the client computer are closed without saving.	N/A
Symantec Management Agent fails to upgrade from Symantec Management Platform 7.1 MP1 to 7.1 SP1.	The Symantec Management Agent fails to upgrade from Symantec Management Platform 7.1 MP1 to 7.1 SP1. The download process starts, the installation service runs, and the new files are put in place. However, the agent service is removed and not put in place again, even though the AltirisAgentInstallation.log reports that the upgrade is successful.	N/A

Table 1-17 Fixed issues for Software Management Framework

Issue	Description	Article link
The **Detection rule** and **Applicability rule** for a software resource do not have an option to delete.	An option to delete is not included on **Detection rule** and **Applicability rule** on the **Software resource: Rules** tab. As a result, these rules are still included in the list of items of a deleted software resource.	N/A
Software Discovery and **Collect Inventory** policy do not support large files.	Software Discovery and the **Collect Inventory** policy cannot handle files larger than 2GB.	N/A
During differential replication, child resource associations are loaded incorrectly.	During differential replication, child resource associations are loaded as parent resource associations. Instead, child resource associations should be loaded so that they remain child resource associations after replication.	N/A
Repeat scheduling does not work in **Managed Software Delivery** policies.	If you create a **Managed Software Delivery** policy and schedule the compliance check to run more frequently than once an hour, the policy may not run repeatedly. However, by default every hour Software Management Framework wakes up any policies that failed to run and triggers their execution.	N/A

Table 1-17 Fixed issues for Software Management Framework *(continued)*

Issue	Description	Article link
Software Catalog and Software Library settings do not replicate.	Changes that are made to any of the settings that are found in **Software Catalog** and the **Software Library Settings** folder are not replicated when a **Replicate now** or **Replicate to** method of replication is invoked.	N/A

Table 1-18 Fixed issues for Credential Manager, Connection Profiles, and the Pluggable Protocols Architecture

Issue	Description	Article link
Impossible to perform monitoring using WMI, HTTP, and SNMP protocols.	Monitoring fails to resolve credentials from Credential Manager with Inner exception. You must enable WCF Activation to allow for using protocols other than HTTPS.	TECH140507
After a Pluggable Protocols Architecture (PPA) upgrade, the WS-MAN protocol is disabled and all settings are set to default.	The WS-MAN protocol is disabled and all settings are set to default after an upgrade to PPA SP4 7.0.7416. To work around this issue, manually enable the WS-MAN protocol, specify custom credentials from the drop-down menu, and reset all settings.	N/A

Table 1-19 Fixed issues for UNIX/Linux/Mac

Issue	Description	Article link
Push installation can fail.	A Push installation of the Unix/Linux/Mac agent can fail with the following message: The ‘cd’ command failed.	N/A
Active user change notification does not work in Unix/Linux/Mac.	Currently, the Unix/Linux/Mac agent does not support user-based policies; therefore, a policy is not executed on user login. The schedule type **At user login** is supported for the Mac platform only.	N/A

Table 1-20 Fixed issues for Symantec Management Console enhanced views

Issue	Description	Article link
Dollar values are not updated when a legacy software license is migrated.	When you migrate a legacy software license, you can choose to migrate the cost of the software. However, the dollar values were not updated. Now, the dollar value of the software appears in the **Software Product License and Usage** section of the **Software** view.	N/A
Licenses that are added using Asset Management Solution do not appear in the **Licenses** tab of the **Add Software Product** dialog box.	You can add a software license to software using Asset Management Solution. However, these licenses did not appear in the **Add Software Product** dialog box. Now, the software license and associated purchase information is added to the **Licenses** tab in the **Software Product** dialog box. The **Software Product** dialog box appears when you click **Manage Licenses** in the **Software Product License and Usage** section of the **Software** view for an installed software product.	N/A
Documentation describes incorrect location for the **Enhanced Views Settings** dialog box.	The product documentation described an incorrect location for the **Enhanced Views Settings** dialog box. Now, the topic "Configuring the Symantec Management Console enhanced views settings" contains the correct information about the location of the **Enhanced Views Settings** dialog box. To access this dialog box, on the **Settings** menu, click **Console > Enhanced Views**.	N/A
Cannot drag and drop with organizational groups and organizational views.	The drag-and-drop functionality did not work with organizational groups and organizational views. Now, when you click **Computers** on the **Manage** menu, you can drag and drop organizational groups onto organizational views.	N/A
Performance and usability issues occur with saved searches in the **Software** view and the **Computers** view.	The performance and usability of the saved searches was slow to refresh. In addition, the flipbook did not always display the correct details for the selected product. Now, this issue is fixed. For example, on the **Manage** menu, click **Software**. On the **Software** view page, click **Installed Products** and then in the center pane (list pane), select a product. You can use the arrow keys on your keyboard to scroll quickly up and down the list, and you can stop on a different product.	N/A

Table 1-20 Fixed issues for Symantec Management Console enhanced views *(continued)*

Issue	Description	Article link
The enhanced console views user interface does not accommodate non-Symantec **Administrator Roles**.	The enhanced console views user interface did not accommodate non-Symantec **Administrator Roles**. Now, this issue is fixed. For example, on the **Settings** menu, click **Security > Account Management**. Expand the **Account Management** folder and click **Roles**. Select a role and click **Privileges**. The following **Software Management** privileges were added: ■ **Create software products** ■ **Define software product inventory filters** ■ **Configure software usage and tracking** ■ **Create software licenses** The following **Software Management Framework Privileges** were added. ■ **Manage Software Resources**	N/A
Searches fail to run when you use the IP criteria as a filter to search for computers in the **Computers** view.	Searches did not run when you used the IP criteria filter to search for computers in the center pane (list pane). Now, this issue is fixed. For example, on the **Manage** menu, click **Computers** . On the **Computers** view page, click **All Computer Views > All Computers**. In the center pane (list pane), click the double-arrows next to the search field. Click **Add Search Criteria > IP Address**. You can use the IP criteria filter to search for computers in the center pane (list pane).	N/A
Internet Explorer Security often asks for your credentials when you use Symantec Management Console.	After you entered the correct credentials, the dialog box did not disappear; instead, it asked you to enter the credentials again and again.	N/A

Table 1-20 Fixed issues for Symantec Management Console enhanced views *(continued)*

Issue	Description	Article link
In the **Add Software Products** dialog box on the **Licenses** tab, you cannot create an additional license for a software product.	You were unable to create an additional license for a software product from the **Add Software Products** dialog box. Now, this issue is fixed. For example, on the **Manage** menu, click **Software**. On the **Software** view page, click **Installed Software > Installed products**. In the center pane (list pane), select a software product. In the right pane (details pane), click **Manage Licenses**. On the **Licenses** tab in the **Software Product** dialog box, click **Add License Purchase**. Under **Software License**, modify the name. Under **Software Purchase**, modify the information.	N/A
When navigating to **Manage > Computers** in the console, the computers and organizational views do not load.	After running an Active Directory Import or creating a large number of organizational groups with Active Directory Connect and then navigating to **Manage > Computers** in the console, the computers and organizational views did not load.	N/A
Operators are not displayed in the drop-down list when you add other values, use search operators, and save the search in the **Computers** view.	When you added other values, used search operators, and saved the search in the **Computers** view, the drop-down list did not display the operator. Now, this issue is fixed. For example, on the **Manage** menu, click **Computers**. On the **Computers** view page, click **All Computer Views > All Computers**. In the center pane (list pane), click the double-arrows next to the search field. Click **Add Search Criteria** and select criteria. Type the OR (|) operator in the box, and save the search. The operators are displayed in the drop-down list.	N/A
Using additional search criteria in the **Computers** view in a non-English-language operating system yields an error.	If you used additional search criteria in the **Computers** view in a non-English-language operating system, an error occurred. Now, this issue is fixed. For example, on the **Manage** menu, click **Computers**. On the **Computers** view page, click **All Computer Views > All Computers**. In the search field in the center pane (list pane), type **"sma"** to narrow the results to **"sma-test"**.	N/A

Other things to know

The following are things to know about this release. If additional information about an issue is available, the issue has a corresponding Article link. Click the link to learn more.

The other things to know about this release are separated into the following components:

- Symantec Installation Manager
  See Table 1-21 on page 40.
- Notification Server
  See Table 1-22 on page 42.
- Task Server
  See Table 1-23 on page 46.
- Software Management Framework
  See Table 1-24 on page 47.
- Network Discovery
  See Table 1-25 on page 50.
- UNIX/Linux/Mac
  See Table 1-26 on page 50.
- Symantec Management Console enhanced console views
  See Table 1-27 on page 52.

Table 1-21 Things to know about Symantec Installation Manager

Issue	Description	Article Link
Maximum length of computer name.	The maximum length of the name of the computer on which Symantec Management Platform is installed is 64 characters.	TECH175694
In-use license count vs. actual license count.	On the **Product Licensing** page, the **In-use** license count can display a misleading number. The number that is displayed may be smaller than the number of licenses that are in use. This error can occur if some client computers are in sleep mode or are turned off.	TECH175697

Table 1-21 Things to know about Symantec Installation Manager *(continued)*

Issue	Description	Article Link
Two migration package files include the word "silent" in their name.	The migration wizard installation package is installed at Program Files\Altiris\Symantec Installation Manager\MigrationPackage. The **MigrationPackage** folder contains four files. Two of these files include the word "silent" in their name. Use the migration package files that do not contain the word "silent" to install the migration wizard.	N/A
Command for setting up the required Internet Information Services (IIS) settings.	To set up the required IIS settings on the server before you install the Symantec Management Platform products, run the following command from the command prompt. `ServerManagerCmd.exe -install Web-WebServer AS-Web-Support Web-Mgmt-Compat Web-Asp NET-HTTP-Activation NET-Non-HTTP-Activ`	N/A
User requirements for migrating Notification Server data to Symantec Management Platform 7.1.	If the logged-on user is not a member of the Local Administrator group, the data migration wizard does not work.	TECH41187
Requirements for installing Symantec Installation Manager.	You cannot install Symantec Installation Manager if the computer does not have a **Temp** folder.	TECH41182
Modify option on the **Installed Products** page is disabled.	The ability to modify an installation is not supported in the current release of Symantec Installation Manager.	TECH41306
Number of applied licenses cannot be reduced.	You cannot reduce the number of licenses that are applied to a product.	TECH41584
Symantec Installation Manager rejects some 6.x licenses.	Symantec Installation Manager does not support the license files that contain multiple certificates.	TECH41323

Table 1-21 Things to know about Symantec Installation Manager *(continued)*

Issue	Description	Article Link
Relaunching Symantec Installation Manager after canceling the migration wizard opens the **Optional Installs** page.	This error can occur when you perform an on-box upgrade. The behavior can occur if you perform both of the following actions: ■ You do not select any of the items on the **Optional Installs** page. ■ You cancel the installation when the migration wizard starts. Symantec Installation Manager opens to the **Optional Installs** page the next time it starts. To determine which products to install, click **Back** to access the **Install New Products** page. Another option is to click **Next** to access the **End User License Agreement** page.	N/A
Symantec Workflow is installed with Symantec Management Platform.	When you install Symantec Management Platform through Symantec Installation Manager, the Symantec Workflow Installer becomes available in the console. In the console, navigate to **Manage > Workflows** to access the Workflow Installer.	DOC4796
Workflow servers are not uninstalled when you uninstall Symantec Management Platform.	When you uninstall Symantec Management Platform, Workflow servers are not uninstalled. You have to uninstall Workflow servers manually.	DOC4796

Table 1-22 Things to know about Notification Server

Issue	Description	Article Link
Three-tier hierarchies are not supported.	Symantec does not support three-tier hierarchies at this time.	HOWTO44217
You must configure Web controls to support ActiveX.	Errors can occur if Internet Explorer settings prevent the ActiveX control from running. For example, the pop-up dialog box is blank when you select the **Edit/New** icon in the **Update summary data** dialog box. For Notification Server to run properly, you must be able to install (or be prompted to install) ActiveX objects. Otherwise, you may see errors with jobs and tasks, among other functions. This function is by design.	N/A

Table 1-22 Things to know about Notification Server *(continued)*

Issue	Description	Article Link
Take care when using the **Query Builder** in Basic mode.	When you modify a report query using **Query Builder** in Basic mode, be careful when you change the first condition of a filter expression. When you change the first condition, the operator drop-down list reloads its contents. You might need to re-select the correct operator to successfully resolve the report query. Note that such unresolvable filter expressions are shown as “Blue” in the Query Builder.	N/A
The **Manage Computers** list sometimes shows duplicate entries of the same computer after SOI task.	This behavior is expected if the name of a computer changes at the same time as its MAC address or its BIOS unique identifier. In this scenario, the computer cannot be identified as the same computer. This issue is common for virtual machines because by default they use randomly generated MAC addresses, which can change. Workaround: Ensure that all virtual machines have statically defined MAC addresses before you change the computer name or domain.	N/A
Windows 2000 clients are not upgraded when you upgrade to Symantec Management Platform 7.1.	Windows 2000 clients that have the 6.x Altiris Agent are not upgraded. This function is by design: Windows 2000 is not supported in Symantec Management Platform 7.1.	N/A
You cannot add domain groups to Symantec Management Platform Security roles.	If you attempt to add a domain user to a security role from **Settings > Security > Roles > Membership**, error message is displayed on the **Add User** dialog box. This error occurs because adding domain groups directly to a security role is no longer a supported scenario. Symantec Management Platform 7.1 only supports adding a Symantec Management Platform role or a Symantec Management Platform account to a role.	TECH144089

Table 1-22 Things to know about Notification Server *(continued)*

Issue	Description	Article Link
Database upgrades cannot be performed across different collations.	If you attempt to upgrade across collations, the database reconfiguration fails with the following error message: Cannot resolve the collation conflict. The database and the database server collations must match. This function is by design: Symantec Management Platform does not support upgrading across different collations.	N/A
Symantec Management Agent icon may not be removed when the Symantec Management Agent is uninstalled.	When you uninstall the Symantec Management Agent from a Windows 7 computer, the Symantec Management Agent icon is not removed. The Symantec Management Agent icon remains listed in the **Customize Icons** list. To view the **Customize Icons** list on a Windows 7 computer, do one of the following: ■ Right-click the taskbar and then click **Properties > Customize**. ■ Click **Show hidden icons** on the toolbar.	TECH44030
Symantec Management Agent icon may not appear in the system tray.	When you install the Symantec Management Agent, you can choose to display the Symantec Management Agent icon in the system tray on the client computer. However, on Windows 7 computers, the Symantec Management Agent icon does not appear in the system tray.	TECH44034
Attempting to add data classes to a new resource type can fail with a script error.	If you create a new resource type and then click **Add Data Classes** on the **Resource Type Edit** page, a script error message is displayed. From the left pane, this error message is also displayed when you click **Settings > Notification Server > Resource and Data Class Settings > Resource Types > Asset Types** and then right-click **New > Resource Type**. Note that you must have CMDB Solution installed to access the **New Resource Type** page. This issue is related to your Internet Explorer browser configuration. The configuration can prevent the necessary ActiveX control from loading. You must enable the data class picker (the AexTreeCtrl ActiveX control) to load successfully. To enable the picker, you must enable automatic prompting for ActiveX controls under the Internet Explorer security settings.	TECH46224

Table 1-22 Things to know about Notification Server *(continued)*

Issue	Description	Article Link
Package Replication Solution does not work on Notification Server 7.1.	The package replication rules that were created using Package Replication Solution on Notification Server 6.0 SP3 cannot be upgraded to equivalent rules in Notification Server 7.1. Errors appear when you attempt to use the package replication importer that is found in the migration wizard.	TECH41330
If the Symantec Management Agent uses a proxy server, the Client Task Agent may fail to register.	When the Symantec Management Agent uses a proxy server, it fails to post events to Notification Server correctly. This failure results in the Client Task Agent not being registered. This error does not affect the communication that involves configuration updates, basic inventory, package snapshot downloads, or package downloads.	TECH41484
The user name for the Symantec Management Agent Connectivity Credential (ACC) cannot include any special characters.	The user name for the Symantec Management Agent ACC cannot include any special characters	TECH41492
In some circumstances the Symantec Management Console displays the **Resource Manager** portal page.	If you open the Resource Manager while the Symantec Management Console is open and then refresh the console page, the console displays the **Resource Manager** portal page. To restore the original page in the Symantec Management Console, you need to select the menu option that you selected previously.	TECH41499
NSSetup.aspx is no longer a supported method for reconfiguring the database from a corrupted console.	Symantec Installation Manager does not support NSSetup.aspx as a method for reconfiguring the database from a corrupted console. To reconfigure the database from a corrupted console, use the `AeXconfig /configureall` command.	HOWTO9821

Table 1-22 Things to know about Notification Server *(continued)*

Issue	Description	Article Link
Track role deletion is now on by default.	The functionality of TrackRoleDeletionForHierarchy is now turned on by default. If you want to turn off track role deletion, contact technical support. (With Symantec Management Platform 7.0 SP5, the following were added to CoreSetting.config:SyncRoleMembershipExactlyDuringReplication and TrackRoleDeletionForHierarchy. With Symantec Management Platform 7.1, TrackRoleDeletionForHierarchy was removed from CoreSetting.config.)	N/A
If SSL is used to access the Symantec Management Platform, additional configuration is required before you can roll out the Symantec Management Agent.	During installation of the Symantec Management Platform products, if you select the **Use SSL for accessing management platform** option on the **Notification Server Configuration** page, then you must install a self-signed certificate on your client computers. You must install the certificate before you deploy the Symantec Management Agent to these computers. You can use an Active Directory group policy to install the certificate before the agent rollout.	N/A

Table 1-23 Things to know about Task Server

Issue	Description	Article Link
Task Server is not supported on a domain controller.	Installation of a Task Server on a Microsoft domain controller is not supported. Installation of a package server on a Microsoft domain controller is supported but not recommended.	HOWTO59071
Upgrade of the Task Server fails because missing or wrong version of .NET Framework.	If you apply a **Legacy Task Server upgrade policy** to the remote Task Server, it can fail to upgrade. The .NET Framework needs to be updated to 3.5 version. This .NET update needs to be done manually before you can upgrade the Task Server. To upgrade the Task Server, you must modify the **Task server legacy upgrade policy.** Make sure that **Run once ASAP** is unchecked but that **User could run** is checked. Then apply the upgrade policy to the remote Task Server.	N/A

Table 1-23 Things to know about Task Server *(continued)*

Issue	Description	Article Link
Pop-up dialog box is blank when you select the **Edit/New** icon in the **Update summary data** dialog box.	For Notification Server to run properly, you must be able to install (or be prompted to install) ActiveX objects. If your Internet Explorer settings prevent the ActiveX control from running, you see errors when you work with jobs and tasks. This function is by design.	N/A
Replication of tasks and task instances in a hierarchy is inconsistent.	Tasks and instances are sometimes replicated immediately when the task is run. Other times tasks and instances are not replicated until the hierarchy schedules run.	N/A
System.Net.Sockets.SocketException occurs when you try to restart the Task Server services (Altiris Object Host service).	In some cases the agent cannot register with Task Server, which prevents users from running tasks on agent computers. For more information, see http://support.microsoft.com/kb/960718.	N/A
A window is not displayed when cmd.exe is running in Task Manager as System.	This error occurs even though the **Show Script in a Normal Window** option is selected. The cause of this error may be a new Windows 2008 security feature called "Session isolation".	N/A
Extra steps are required when you install Task Server in Internet Information Services 7.0.	Extra steps are required to install Task Server on computers running Windows 2008 or 7. These steps include enabling certain options when you install the Web services role and running a specific command before you install Task Server.	HOWTO47804

Table 1-24 Things to know about Software Management Framework

Issue	Description	Article Link
Terminology documented.	A list of the terminology that is used in Software Management Framework is available.	DOC1717

Table 1-24 Things to know about Software Management Framework *(continued)*

Issue	Description	Article Link
Software Management Framework documentation was updated for enhanced console views.	With the enhanced console views, the **Software Catalog** page was replaced with a **Software** view. The **Software** view has new functionality that was not part of the **Software Catalog** page. In addition, some of the functionality that was on the **Software Catalog** page is now accessed from the **Manage Software Catalog** window. Because the enhanced console views introduced these changes, the Symantec Management Framework documentation was updated. If you do not have the enhanced console views installed, Symantec recommends that you use the *Symantec Management Platform 7.1 MP1 User Guide* for the topics that deal with the Software Catalog. The user guide is available at http://www.symantec.com/docs/doc3722. The enhanced console views are installed if you have Deployment Solution installed either as a standalone product or as part of a suite. For more information about enhanced console views, see *Altiris IT Management Suite 7.1 from Symantec Enhanced Console Views Getting Started Guide*. This guide is available at http://www.symantec.com/docs/doc3563.	N/A
References to software component or software resource are added.	If you have the enhanced console views installed, the **Manage Software Catalog** window refers to software components. A software component is the same thing as a software resource.	N/A
Symantec does not support the creation of software packages under the **Program Files\Altiris\Notification Server** folder.	Symantec does not support the creation of software packages under the **Program Files\Altiris\Notification Server** folder. Microsoft recommends that you not place any files under **Program Files**. This location should only contain the files that are installed during the installation of an application. For backward compatibility, Symantec still supports storing software packages under **Program Files\Altiris\Notification Server\NSCap**.	TECH176459
Java runtime is required for importing packages into the Software Management Framework.	If JRE 1.6 or higher is not installed, an error message appears when you try to import or add a package to the Software Management Framework.	HOWTO9940

Table 1-24 Things to know about Software Management Framework *(continued)*

Issue	Description	Article Link
Accessing the Symantec Management Console remotely can cause some Software Catalog functions not to work.	The loss of functionality occurs if you access the console remotely from a computer that is not part of the Notification Server computer admin domain.	TECH127274
Replicating a single resource does not replicate dependent resources.	When you replicate a single resource, any dependent resources are not automatically replicated. If you want dependent resources to be replicated, you must replicate them as well. If you replicate a Managed Software Delivery policy that has a detection rule, you must also replicate the detection rule. If you do not replicate the rule, the policy fails.	TECH46168
Turning on a computer with a Managed Software Delivery policy works only when it is first enabled and saved.	When you schedule a Managed Software Delivery policy, the **Power on if necessary** option turns on a client computer only when the policy is initially enabled and saved. It does not wake up a client computer after the policy is on the client computer.	N/A
The description of a data provider task does not identify the task until the task runs.	If you create a new schedule for a data provider task that includes a description and you schedule the task to run in the future, the task is only identified when it runs.	N/A
A Quick Delivery task does not execute in Hidden mode for an EXE.	A task may not execute in Hidden mode when you perform both of the following actions: ■ You deliver an EXE file with a Quick Delivery task. ■ You select **Hidden** in the **Display** window drop-down list on the **Run Options** tab of the **Advanced** options. The installation is hidden if the EXE obeys the request to hide the installation.	N/A
Symbolic links are lost if TAR/TAR.GZ/TAR/Z packages are unzipped or repackaged on a Windows computer.	To preserve symbolic links, do not unzip or repackage these packages on a non-UNIX computer.	N/A

Table 1-25 Things to know about Network Discovery

Issue	Description	Article Link
Using the connection profiles that Network Discovery tasks use.	Use connection profiles to configure the protocols that are used to communicate with network devices.	HOWTO9348
Importing .MIB files on Symantec Management Platform 7.0.	You can import .MIB files to Symantec Management Platform 7.0.	HOWTO9709
Setting up Symantec Management Platform Security Privileges.	You can set up Symantec Management Platform Security Privileges.	DOC1740
Scheduling a Network Discovery task.	If you schedule a Network Discovery task to run on a recurring basis, you cannot stop that task unless you perform one of the following actions: ■ Delete the task. ■ In the console, under **Manage > Jobs and Tasks**, delete the next scheduled occurrence of the task. This action cancels the schedule.	N/A

Table 1-26 Things to know about UNIX/Linux/Mac

Issue	Description	Article Link
Supported Mac operating systems.	Symantec supports Apple OS X up to and including the Snow Leopard release.	
Unix/Linux/Mac agent cannot be installed on HP-UX if CSH is set as root shell.	When you push-install the Unix/Linux/Mac agent onto the HP-UX computers that have CSH set as boot-shell for root, links to the agent's binaries location (commands) are created. However, on systems such as HP-UX ia64 11.23-11.31, these binaries or commands cannot be executed in user sessions. In this case, you must specify the absolute path.	TECH133272

Table 1-26 Things to know about UNIX/Linux/Mac *(continued)*

Issue	Description	Article Link
Legacy 6.x SWD tasks may ignore scheduling and execute as soon as they arrive on Unix/Linux/Mac 7.1 client systems.	The **Run once ASAP** option may be checked in the legacy SWD task. This option supersedes any scheduled time or maintenance window. This function is by design. If you do not deselect this option, the software delivery task is executed as soon as a policy arrives on the client systems and overrides any schedule. When you add schedules to a Legacy Software Delivery task, uncheck the **Run Once ASAP** option. The only exception is if you intend the task to execute at the first opportunity.	N/A
Push-installing the Symantec Management Agent for UNIX, Linux, and Mac to a computer that has the secondary shell configured in .profile may fail with timeout errors.	If you attempt to push-install the Symantec Management Agent for UNIX, Linux, and Mac to a computer system that has a secondary shell that is configured in .profile, the installation may fail. The failure is due to a timeout error. The secondary shell is any shell other than the configured shell in `/etc/passwd` for user root in `/etc/profile`, `.profile`, or `.bash_profile`.	TECH44831
Installing the Symantec Management Agent for UNIX, Linux, and Mac on an HP-UX 11.00 computer produces a “Memory fault (coredump)” error.	This issue is due to a defect in the dynamic linker on the HP-UX 11.00 computer. You need to apply the appropriate patch.	TECH42006
Daemons running on Mac 10.6 in root bootstrap context cannot execute commands using the `nohup` utility.	This issue is a system limitation that is caused by Mac OS 10.6 operating system design, and it cannot be overridden. This limitation may affect the commands that SWD/SMF tasks execute, or it may affect Script tasks.	TECH47689
Managed and quick software deliveries may fail on some HP-UX systems.	Managed deliveries and quick software deliveries that contain a tar.bz2 or .bz2 related command line may fail on some HP-UX systems.	TECH137859

Table 1-26 Things to know about UNIX/Linux/Mac *(continued)*

Issue	Description	Article Link
You must include a trailing slash to specify an alternate download location for a Linux package server.	A package server configuration has an **Alternate Download Location** option. With a Linux package server, you can set this option with a Windows-style path. The path is then converted to a UNIX-style path; for example, `C:\path\` becomes `/path/`. However, a trailing slash is required for proper conversion. If you omit the trailing slash as in `C:\path`, then the path is not converted correctly.	N/A

Table 1-27 Things to know about Symantec Management Console enhanced views

Issue	Description	Article Link
Enhanced console views installed with specific products.	Enhanced console views are installed with Deployment Solution. Deployment Solution is included with complete installations of Client Management Suite, Server Management Suite, IT Management Suite, and standalone Deployment Solution. If Deployment Solution is not installed as a standalone, or if Deployment Solution is deselected from any suite installation, enhanced console views are not installed.	N/A
Process for updating to enhanced console views 7.1 SP2 from a 7.1 SP1 environment that includes installed hot fixes.	Verify that you have an environment that includes installed hot fixes (HF1 or HF2). In Symantec Installation Manager on the **Installed Products** page, click **View and install updates**. If you do not find **Altiris Deployment Solution Complete Suite 7.1 SP1aMR1a** in the list of updates on the **Product Updates** page, then you have an environment that includes installed hot fixes. You must use the **Install new products** option in Symantec Installation Manager to update to enhanced console views 7.1 SP2.	HOWTO61133

Table 1-27 Things to know about Symantec Management Console enhanced views *(continued)*

Issue	Description	Article Link
Process for updating to enhanced console views 7.1 SP2 from a 7.1 SP1 environment that does not include installed hot fixes.	Verify that you have an environment that does not include installed hot fixes (HF1 or HF2). In Symantec Installation Manager on the **Installed Products** page, click **View and install updates**. If you find **Altiris Deployment Solution Complete Suite 7.1SP1aMR1a** in the list of updates on the **Product Updates** page, then you have an environment that does not include installed hot fixes. In Symantec Installation Manager, use the **View and install updates** option to update to enhanced console views 7.1 SP2. You must select the **Altiris Deployment Solution Complete Suite 7.1 SP1a MR1a** update.	N/A
Enhanced console views appear in Symantec Management Console.	Enhanced console views appear when you select any of the following from the **Manage** menu: ■ **Computers** ■ **Software** ■ **Software Catalog** ■ **Jobs and Tasks** ■ **Policies**	N/A
A managed software product can have up to 99 software components, and each component can have up to 20 EXEs.	When the enhanced console views are installed, you can manage software products. Enhanced console views support up to 99 software components per managed software product and up to 20 EXEs per software component.	N/A

Documentation that is installed

Table 1-28 Documentation that is included in the product installation

Document	Description	Location
Help	Information about how to use this product. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. Context-sensitive help is available for most screens in the Symantec Management Console. To open context-sensitive help, click inside the window, pane, dialog box, or other screen element about which you want more information, and then do one of the following: ■ Press the F1 key. ■ In the Symantec Management Console, click **Help > Context**. In the **Symantec Help Center** window, type your search string to search within the installed documentation. To expand your search to the Symantec Knowledge Base, check **Include online search**. For more information on how to use the **Symantec Help Center**, click the **Home** symbol.
User Guide	Information about how to use this product. This information is available in PDF format.	■ The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. The Documentation Library provides a link to the PDF User Guide on the Symantec support Web site. ■ The **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Documentation**.

Other information

Table 1-29 Information resources that you can use to get more information

Document	Description	Location
ITMS 7.1 SP2 Planning and Implementation Guide	Information about capacity recommendations, design models, scenarios, test results, and optimization best practices to consider when planning or customizing ITMS.	http://www.symantec.com/docs/DOC4827

Table 1-29 Information resources that you can use to get more information *(continued)*

Document	Description	Location
Symantec Management Platform User Guide	Information about using the Symantec Management Platform.	Symantec Management Platform Documentation page
Symantec Management Platform Installation Guide	Information about using Symantec Installation Manager to install the Symantec Management Platform products.	http://www.symantec.com/docs/DOC4798
Knowledge base	Articles, incidents, and issues about this product.	SymWISE support page
Symantec Connect	An online magazine that contains best practices, tips, tricks, and articles for users of this product.	Symantec Connect page